



Daily Open Source Infrastructure Report 18 November 2016

Top Stories

- Twelve individuals were charged November 16 for their alleged roles in an ATM skimming scheme that defrauded Bank of America and PNC Financial Services Group, Inc. customers in New Jersey out of more than \$428,000. – *U.S. Department of Justice* (See item [3](#))
- The Hawaii State Department of Health’s Clean Water Branch reported that around 4,275 gallons of raw sewage entered a storm drain at Lake Wilson in Wahiawa November 15. – *Honolulu Star-Advertiser* (See item [12](#))
- North Carolina officials reported November 17 that hundreds of fire personnel were working to contain dozens of wildfires that have scorched a total of roughly 49,112 acres across the State. – *WNCN 17 Goldsboro; Associated Press* (See item [14](#))
- A Whittier, California resident was convicted November 16 for his role in a scheme where he and 3 co-conspirators defrauded Electronic Arts (EA) out of more than \$16 million. – *U.S. Department of Justice* (See item [20](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. *November 17, Peoria Journal Star* – (Illinois) **Ameren worker killed in large gas explosion in downtown Canton.** A natural gas explosion in Canton, Illinois, killed 1 person and sent at least 11 others to an area hospital November 16. Ameren Illinois officials reported the explosion occurred while crews were making repairs to a gas leak in an area building.
Source: <http://www.pjstar.com/news/20161116/ameren-worker-killed-in-large-gas-explosion-in-downtown-canton>
2. *November 16, Union Missourian* – (Missouri) **Gerald gas leak cleanup continues.** Crews continued working November 16 to clean up more than 250 barrels of fuel that spilled near Gerald, Missouri, November 12 after the 24-inch Explorer Pipeline leaked inside a pump station. Crews have already removed more than 10,000 gallons of gas and officials reported the spill was contained before it reached any streams or drainage ditches.
Source: http://www.emissourian.com/local_news/county/gerald-gas-leak-cleanup-continues/article_762c5136-443d-5607-8221-4495dd485a94.html

Chemical Industry Sector

See item [10](#)

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *November 16, U.S. Department of Justice* – (New Jersey) **Twelve individuals charged in ATM skimming conspiracy.** Twelve individuals were charged November 16 for their alleged involvement in an ATM skimming scheme that defrauded Bank of America and PNC Financial Services Group, Inc. customers in New Jersey out of more than \$428,000 between March 2015 and July 2016. The group reportedly installed skimming devices on ATMs at banks across New Jersey to record payment card data encoded on the magnetic stripe of credit and debit cards, and transferred the stolen information onto counterfeit bank cards that they subsequently used to withdraw cash from the affected accounts.
Source: <https://www.justice.gov/opa/pr/twelve-individuals-charged-atm-skimming->

[conspiracy](#)

4. *November 16, U.S. Department of Justice* – (National) **Two Tennessee residents indicted for conspiracy and employment tax fraud.** Two Tennessee residents were charged in an indictment unsealed November 15 after the pair allegedly conspiring to defraud the U.S. Internal Revenue Service (IRS) by neglecting to collect and pay roughly \$2.8 million in employment tax while running a temporary staffing company serving firms in Tennessee and elsewhere, failing to timely file employment tax returns, and filing false employment tax returns, among other fraudulent actions. The charges also allege that the duo falsely represented to the IRS their management of the company and knowledge of their responsibility to honestly account for and pay out employment taxes, placed the company in the names of nominees with no control over business operations, and established payment arrangements to impede an IRS levy placed on their customer payments.
Source: <https://www.justice.gov/opa/pr/two-tennessee-residents-indicted-conspiracy-and-employment-tax-fraud>

Transportation Systems Sector

5. *November 17, WWSB 40 Sarasota* – (Florida) **Pig carcasses spill onto I-75 causing traffic delays.** A vehicle transporting animal remains spilled its load onto the northbound lanes of Interstate 75 near Fruitville Road in Sarasota, Florida, November 16, prompting the closure of 2 lanes for several hours while crews worked to clean-up the carcasses.
Source: http://www.mysuncoast.com/news/local/update-all-lanes-reopen-after-pig-carcass-spill-on-i/article_fc1f3f08-ac03-11e6-8d7f-ff71302786c6.html
6. *November 16, Fox News; Associated Press* – (Oklahoma) **Gunman ID'd in deadly Oklahoma City airport shooting.** A former Southwest Airlines Co. employee opened fire at Will Rogers World Airport in Oklahoma City November 16 and killed 1 other person before taking his own life, prompting officials to divert all incoming flights and cancel Southwest flights departing from the airport until November 17, and stranding hundreds of people inside the terminal and on the runway for more than 3 hours.
Source: <http://www.foxnews.com/us/2016/11/16/police-search-for-motive-in-killing-airport-worker.html>
7. *November 16, WCCO 4 Minneapolis* – (Minnesota) **Hwy 7 closes after massive tank falls off semi.** Minnesota State Patrol officials closed Highway 7 in Victoria until at least November 17 after a semi-truck carrying a 368,000-gallon tank lost its load November 16, spilling diesel fuel and hydraulic fluids on the roadway. Crews built a crane to lift the tank onto a trailer and were working to determine the cause of the accident.
Source: <http://minnesota.cbslocal.com/2016/11/16/hwy-7-excelsior-closure/>
8. *November 16, Salem Statesman Journal* – (Oregon) **Dallas man dies in early morning crash on Highway 223.** Highway 223 near Dallas, Oregon, was closed for 7 hours November 16 following a multi-vehicle collision that killed 1 person and injured another. The cause of the crash remains under investigation.

Source: <http://www.statesmanjournal.com/story/news/2016/11/16/dallas-man-dies-early-morning-crash-highway-223/93988742/>

Food and Agriculture Sector

9. *November 17, Spokane Spokesman-Review* – (Idaho) **Clearwater steelhead go belly up below Dworshak Dam.** The U.S. Army Corps of Engineers reported that roughly 200 dead adult steelhead fish were found in the tailrace below the Dworshak Dam in Clearwater County, Idaho, the week of November 14. A U.S. Fish and Wildlife Service assessment at the Dworshak Fish Hatchery revealed the steelhead deaths likely resulted from contact with structural features of the dam's turbine unit 2.
Source: <http://www.spokesman.com/blogs/outdoors/2016/nov/17/clearwater-steelhead-go-belly-below-dworshak-dam/>
10. *November 16, Napa Valley Register* – (California) **Amy's Kitchen building evacuated after release of disinfectant chemicals.** The Santa Rosa Fire Department in California is investigating after a sodium hydroxide and sodium hypochlorite release at an Amy's Kitchen facility prompted the evacuation of two dozen employees for several hours November 15. A HAZMAT team contained the chemical flow to the building.
Source: http://napavalleyregister.com/news/state-california/amy-s-kitchen-building-evacuated-after-realease-of-disinfectant-chemicals/article_cc1696d7-b1c4-5746-b1d1-1ff529b7591a.html
11. *November 16, U.S. Food and Drug Administration* – (Illinois; Ohio) **The Popcorn Shoppe issues allergy alert on undeclared milk and soy in Olde Tyme Recipe Popcorn Balls, Edwards Orchard Popcorn Balls and Edwards Orchards West Popcorn Balls.** The Popcorn Shoppe issued a voluntary recall November 16 for its Olde Tyme Recipe Popcorn Balls, Edwards Orchard Popcorn Balls, and Edwards Orchard West Popcorn Balls products sold in 4-pack bags after an Ohio Department of Agriculture inspector discovered that the ingredient label failed to declare the presence of milk and soy in the products. No illnesses have been reported and the products were sold at retail outlets in Illinois and Ohio.
Source: <http://www.fda.gov/Safety/Recalls/ucm529501.htm>

Water and Wastewater Systems Sector

12. *November 16, Honolulu Star-Advertiser* – (Hawaii) **More than 4,000 gallons of sewage spills into Lake Wilson.** The Hawaii State Department of Health's Clean Water Branch reported that around 4,275 gallons of raw sewage entered a storm drain at Lake Wilson in Wahiawa November 15. Crews stopped the spill and removed 300 gallons of the discharge, and the Clean Water Branch advised the public to keep away from lake waters between Olive Avenue and the spillway until further notice.
Source: <http://www.staradvertiser.com/2016/11/16/breaking-news/more-than-4000-gallons-of-sewage-spills-into-lake-wilson/>
13. *November 16, Klamath Falls Herald and News* – (California) **Tulelake water project off the ground.** Tulelake Public Works officials and the mayor of Tulelake, California,

officially opened November 15 the city's new \$6.3 million wastewater treatment facility that is equipped with lined storage ponds for better environmental protection and a new pump and blower system that aerates treatment ponds at double the capacity with less than 40 percent of the power.

Source: http://www.heraldandnews.com/news/local_news/tulelake-water-project-off-the-ground/article_4a98f0a0-3b3d-578b-a841-298b1f79bbe9.html

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

14. *November 17, WNCN 17 Goldsboro; Associated Press* – (North Carolina) **NC wildfires near 50,000 acres as Lake Lure fire spreads to evacuated areas.** North Carolina Forest Service officials reported November 17 that hundreds of fire personnel were working to contain dozens of wildfires that have scorched a total of roughly 49,112 acres across the State, including the 5,700-acre Party Rock Fire in Rutherford County that has forced the evacuation of over 1,000 area residents.

Source: <http://wncn.com/2016/11/16/nc-wildfires-near-50000-acres-as-lake-lure-fire-spreads-to-evacuated-areas/>

Emergency Services Sector

Nothing to report

Information Technology Sector

15. *November 17, SecurityWeek* – (International) **Several vulnerabilities patched in Drupal 7, 8.** Drupal released versions 7.52 and 8.2.3 addressing four vulnerabilities including a flaw in Drupal 8 that can be exploited to cause a denial-of-service (DoS) condition with specially crafted URLs via the transliteration mechanism. The updates also resolved a flaw in Drupal 7 that could allow a malicious actor to build a confirmation form Uniform Resource Locator (URL) that redirects victims to third-party Websites after they interact with the form, among other flaws.
Source: <http://www.securityweek.com/several-vulnerabilities-patched-drupal-7-8>
16. *November 17, Softpedia* – (International) **Raspberry Pi-based hacking device can break into any computer in seconds.** A security researcher created a hijacking device, dubbed PoisonTap, which is an inexpensive Raspberry Pi Zero device that leverages a backdoor installed on a targeted device via USB and imitates an Internet over USB connection to convince the computer it is connected via the Ethernet, causing the device to be configured to prioritize the USB connection and begin sending unencrypted Internet traffic to PoisonTap. Once the hacking device hijacks all the Web traffic, it collects Hypertext Transfer Protocol (HTTP) authentication cookies and session data, thereby allowing an actor to bypass two-factor authentication (2FA) and access a user's online accounts.

Source: <http://news.softpedia.com/news/raspberry-pi-based-hacking-device-can-break-into-any-computer-in-seconds-510295.shtml>

17. *November 16, SecurityWeek* – (International) **Firefox 50 patches 27 vulnerabilities.** Mozilla released Firefox 50 to address 27 vulnerabilities including a critical heap-buffer-overflow in the Cairo programming library when processing Scalable Vector Graphics (SVG) content that could lead to a crash due to compiler optimization, as well as a series of critical memory safety issues that could potentially be exploited by a malicious actor to run arbitrary code, among other flaws. The new browser also adds Download Protection for many executable file types on Microsoft Windows, Apple Mac, and Linux to improve overall security for users.
Source: <http://www.securityweek.com/firefox-50-patches-27-vulnerabilities>
18. *November 16, SecurityWeek* – (International) **Backdoor in some Android phones sends data to server in China.** Kryptowire security researchers reported that several Android models sold in the U.S. were found to include a backdoor in their firmware that transmits personal identifiable information (PII) including contact lists, call history, and text messages to third-party servers without the victim's authorization via a commercial Firmware Over The Air (FOTA) update software system managed by Shanghai ADUPS Technology Co. Ltd. The researchers found the firmware could remotely install applications without user consent, target specific users and text messages by matching remotely defined keywords, and collect data on the use of applications on an affected device.
Source: <http://www.securityweek.com/backdoor-some-android-phones-sends-data-server-china>
19. *November 16, SecurityWeek* – (International) **CryptoLuck ransomware emerges.** A Proofpoint security researcher discovered a new ransomware family, dubbed CryptoLuck that leverages the RIG-Empire exploit kit (EK) for distribution, and abuses the legitimate GoogleUpdate.exe executable and dynamic-link library (DLL) hijacking to infect devices. The malware spreads in the form of a RAR self-extracting archive (SFX) file and performs a series of checks to ensure it is not running in a virtual machine before scanning all mounted drives and unmapped network shares for files it can encrypt.
Source: <http://www.securityweek.com/cryptoluck-ransomware-emerges>
20. *November 16, U.S. Department of Justice* – (International) **Fourth defendant convicted in scheme that defrauded software company of over \$16 million worth of virtual currency.** A Whittier, California resident was convicted November 16 for his role in a scheme where he and 3 co-conspirators defrauded software company and FIFA Football video game publisher, Electronic Arts (EA) out of more than \$16 million by creating software that fraudulently logged thousands of FIFA Football matches to circumvent security mechanisms created by the firm and illicitly earn FIFA coins, which the trio subsequently exchanged on a secondary market where the coins are exchanged for dollars. The three co-conspirators previously pleaded guilty for their roles in the scheme.

Source: <https://www.justice.gov/opa/pr/fourth-defendant-convicted-scheme-defrauded-software-company-over-16-million-worth-virtual>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

Communications Sector

Nothing to report

Commercial Facilities Sector

21. *November 16, KGBT 4 Harlingen* – (Texas) **Refrigeration leak prompts evacuation of HEB in McAllen.** The HEB Grocery Company, LP store in McAllen, Texas, was closed until further notice November 16 after a refrigeration leak sent 7 people to the hospital and prompted an evacuation of the store.
Source: <http://valleycentral.com/news/local/refrigeration-leak-prompts-evacuation-of-heb-in-mcallen>
22. *November 16, WCTV 6 Thomasville* – (Florida) **Bomb found in Tallahassee successfully detonated.** Residents of multiple apartment complexes in Tallahassee, Florida, were evacuated for several hours November 16 after a World War II era bomb was found by construction workers. No injuries were reported and the bomb was detonated on-site.
Source: <http://www.wctv.tv/content/news/Bomb-investigation-in-Tallahassee-evacuations-underway-401544306.html>
23. *November 16, KOKH 25 Oklahoma City* – (Oklahoma) **No injuries, three units ‘extensively damaged’ in apartment fire.** A fire caused an estimated \$148,000 in damages to the Woodscape Apartments in Oklahoma City November 16. No injuries were reported and the fire was deemed accidental.
Source: <http://okcfox.com/news/local/evacuations-underway-as-firefighters-battle-apartment-fire>

Dams Sector

Nothing to report



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes .
Removal from Distribution List:	Send mail to support@govdelivery.com .

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.